REMARKS/ARGUMENTS

The present Amendment is in response to the Office Action having a mailing date of February 11, 2005. Claims 1-19 are pending in the present Application. Applicant has added claims 20-22. Consequently, claims 1-22 remain pending in the present Application.

Applicant has added claims 20-22, which recite that key material for a portion of at least two levels are not bound. Support for the amendment can be found in Figure 2B of the present application. Accordingly, Applicant respectfully submits that no new matter is added.

In the above-identified Office Action, the Examiner rejected claims 1-17 under 35 U.S.C. § 103 as being unpatentable over U.S. Patent No. 6,792,113 (Ansell) in view of U.S. Patent Publication No. 2002/0071559 (Christensen). In so doing, the Examiner indicated that Ansell teaches that a security key pair can be associated with either machine binding (bound) or user-binding (not bound). The Examiner indicated that Ansell does not expressly disclose creating key pair material for use with an embedded security chip of a computer system. Consequently, the Examiner relied upon Christensen for this teaching.

Applicant respectfully disagrees with the Examiner's rejection. Claim 1 recites a method for control of key pair usage in a computer system. The method recited in claim 1 includes creating key pair material for utilization with an embedded security chip of the computer system. The key pair material is specifically recited as including tag data. Claim 1 further recites determining whether the key pair material is bound to the embedded security chip based on the tag data. Claim 7 recites an analogous computer system including a main processor and a security processor. The security processor stores tag data with key pair material and determines binding of the key pair material to the security processor based on the tag data. Similarly, claim 16 recites a method for controlling usage of key pairs in a hierarchical structure of key pairs in an

embedded security chip. Claim 16 recites storing tag data with key pair data for each level of the hierarchical structure and determining whether the key pair data is bound to the embedded security chip based on the tag data.

Thus, claims 1, 7, and 16 utilize tag data stored with the key pair material in order to determine the binding status of the key pair. Consequently, a user can either be bound to a particular system or may be verified securely on any system. Specification, page 7, lines 9-13.

Ansell in view of Christensen fail to teach or suggest the methods and system recited in claims 1, 7, and 16. In particular, Ansell in view of Christensen fails to teach or suggest storing tag data along with key material in conjunction with using the tag data to determine whether the key material is bound to the system. The cited portion of Ansell describes the ability of the system of Ansell to change a key pair from a machine-bound (bound) pair to a user-bound (not bound) pair. Ansell, col. 2, lines 28-66. To do so, the keys are stored in passports. However, the history of the keys, including the whether the key/passport has been converted from bound to unbound is stored not in the passport, but in a table in a certificate database. Ansell, col. 10, line 6-64. Applicant respectfully submits, therefore, that data relating to the nature (bound/unbound) of the key resides in the certificate database. Consequently, the cited portion of Ansell indicates that Ansell stores information regarding the binding status of the key, not with the key in the passport, but in the separate certificate database 127. Thus, Ansell fails to teach or suggest storing tag information from which the binding state of the key material can be determined along with the key material.

Christensen fails to remedy this defect. The cited portions of Christensen do describe encryption and decryption, including storing a key material in a processor. However, Applicant has found no mention in the cited portions of Christensen of storing tags with the key material, or that such tags can be used to determine whether the key material is bound. Consequently, any

combination of Ansell and Christensen would also fail to include such a feature. Stated differently, if the system of Christensen were added to the teachings of Ansell, the system of Ansell might use an embedded processor to perform certain aspects of encryption/decryption, including storage of key material. However, the system would still track the status of the passports and, therefore, the key material using the certificates stored in the certificate database. Consequently, Ansell in view of Christensen fail to teach or suggest storing tag data that determines whether the key material is bound along with key material. Ansell in view of Christensen thus fail to teach or suggest the methods and system recited in claims 1, 7, and 16. Accordingly, Applicant respectfully submits that claims 1, 7, and 16 are allowable over the cited references.

Claims 2-6 and 20 depend upon independent claim 1. Claims 8-15 and 21 depend upon independent claim 7. Claims 17-19 and 22 depend upon claim 16. Consequently, the arguments herein apply with full force to claims 2-6, 8-15, and 17-22. Accordingly, Applicant respectfully submits that claims 2-6, 8-15, and 17-22 are allowable over the cited references.

Applicant's attorney believes that this application is in condition for allowance. Should any unresolved issues remain, Examiner is invited to call Applicant's attorney at the telephone number indicated below.

Respectfully submitted,

SAWYER LAW GROUP LLP

May 11, 2005
Date

/Janyce R. Mitchell/ Reg. No. 40,095
Janyce R. Mitchell
Attorney for Applicant(s)
(650) 493-4540